CLIPPEDIMAGE= JP02000181871A
PAT-NO: JP02000181871A
DOCUMENT-IDENTIFIER: JP 2000181871 A
TITLE: DEVICE AND METHOD FOR AUTHENTICATION
PUBN-DATE: June 30, 2000
INVENTOR-INFORMATION:

NAME	COUNTRY
TIMOTHY, ALAN DIETZ	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
INTERNATL BUSINESS MACH CORP <IBM>	N/A

APPL-NO: JP11349691
APPL-DATE: December 9, 1999
INT-CL_(IPC): G06F015/00; G06F019/00 ; G06F017/30 ; H04L009/32
ABSTRACT:

PROBLEM TO BE SOLVED: To enable a safe transaction by decoding a user request into living body measurement data at a remote place by using an open key and confirming biological measurement data in order to authenticate a user request.

SOLUTION: The user inputs living body measurement data (fingerprint, etc.), through a biometric input sensor 62. An encryption processor assembly(EPA) 58 enciphers a combination of biometric data and transaction data by using a key K1 and adds the ID of the EPA 58 to a request message. The message is sent to a credit server 70. The server 70 uses EPAID to retrieve the key K2 of the user associated with a data base 72 and deciphers the message with the key K2. A confirming function 80 retrieves user data from a biometric data base 74 by using the biometric part of the message, makes an authentication decision, and enciphers the replay with the key K2. The server 70 sends the reply to the user.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－181871
（P2000－181871A）
(43)公開日　平成12年６月30日(2000.6.30)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
G06F	15/00	330	G06F	15/00	330F
					330E
	19/00			15/30	330
	17/30			15/40	370Z
H04L	9/32		H04L	9/00	673D

審査請求　有　請求項の数20　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平11－349691

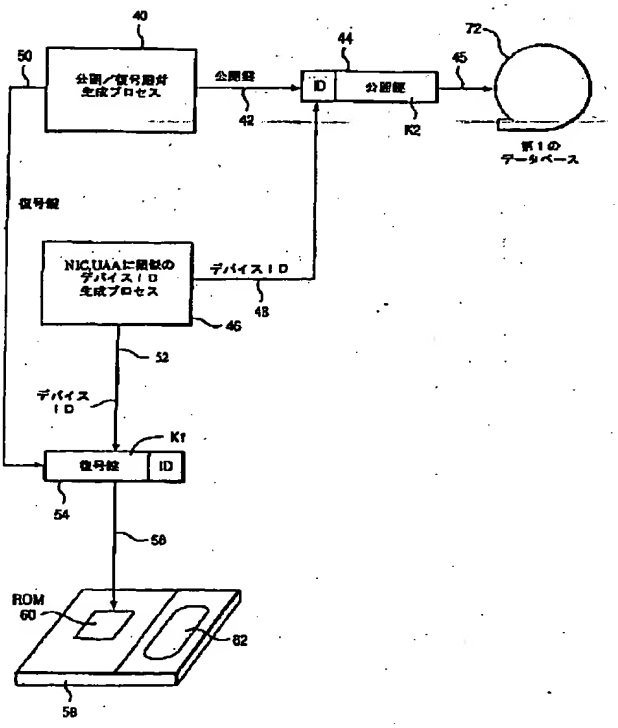
(22)出願日　平成11年12月９日(1999.12.9)

(31)優先権主張番号　０９／２１３３２４
(32)優先日　平成10年12月16日(1998.12.16)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(72)発明者　ティモシー・アラン・ディエツ
アメリカ合衆国78717　テキサス州、　オースティン、　ヴァロナ・ドライブ　10004
(74)代理人　100086243
弁理士　坂口　博　（外１名）

(54)【発明の名称】　認証方法及び装置

(57)【要約】
【課題】　コンピュータ・システムのセキュリティ技術、特に遠隔地からの要求およびメッセージを認証するための方法、装置、およびコンピュータ・プログラム・プロダクトを提供。
【解決手段】方法、装置、およびコンピュータ・プログラム・プロダクトは、復号鍵および公開鍵を生成し、ユーザに対応する生物測定学的データを生成し、遠隔地で生物測定学的データと公開鍵とを記憶し、復号鍵によって暗号化された生物測定学的データを含むユーザ要求を局所で生成し、遠隔地にユーザ要求を伝送し、遠隔地で公開鍵を用いてユーザ要求を生物測定学的データに解読し、記憶された生物測定学的データを検索し、さらにユーザ要求を認証するために生物学的測定データを確認する。



1

【特許請求の範囲】
【請求項１】コンピュータ・システム・ネットワークでユーザの要求を認証するための方法であって、
復号鍵および公開鍵を生成するステップと、
前記ユーザに対応する生物測定データを生成するステップと、
遠隔地で前記生物測定データと前記公開鍵とを記憶するステップと、
前記復号鍵によって暗号化された前記生物測定データを含む前記ユーザ要求を局所で生成するステップと、
前記遠隔地に前記ユーザ要求を伝送するステップと、
前記遠隔地で前記公開鍵を用いて前記ユーザ要求を前記生物測定データに解読するステップと、
前記記憶された生物測定データを検索するステップと、
前記ユーザ要求を認証するために前記生物学的測定データを確認するステップと、
を有することを特徴とする方法。
【請求項２】前記生物学的測定データを確認するステップは、前記解読されたユーザ要求に送られた前記生物測定データと前記記憶された生物測定データとを比較することを含むことを特徴とする請求項１に記載の方法。
【請求項３】前記ユーザ要求の伝送は、前記局所と前記遠隔地とを相互接続するネットワーク上であることを特徴とする請求項２に記載の方法。
【請求項４】前記復号鍵に対応付けられたＩＤ番号を持つ前記遠隔地の前記復号鍵を記憶するステップを、さらに有することを特徴とする請求項３に記載の方法。
【請求項５】前記ＩＤ番号は前記公開鍵に対して一意的に対応付けされており、前記方法はさらに、
前記ＩＤ番号および前記公開鍵を前記遠隔地の第１のデータベースに組として記憶するステップを有することを特徴とする請求項４に記載の方法。
【請求項６】前記生物測定データは第２のデータベースに記憶されていることを特徴とする請求項５に記載の方法。
【請求項７】前記ユーザおよび前記生物測定データに対応付けられたデータ・フィールドを生成するステップと、
前記生物測定データと前記データ・フィールドとを組として前記第２のデータベースに記憶するステップと、
をさらに有することを特徴とする請求項６に記載の方法。
【請求項８】前記復号鍵を記憶するステップは、前記局所で行われることを特徴とする請求項７に記載の方法。
【請求項９】前記生物測定データを生成するステップは、前記局所で行われることを特徴とする請求項８に記載の方法。
【請求項１０】前記確認に応じて前記要求を処理するステップをさらに有することを特徴とする請求項９に記載の方法。

2

【請求項１１】コンピュータ・システム・ネットワークでユーザの要求を認証する装置であって、
復号鍵および公開鍵を生成する手段と、
前記ユーザに対応する生物測定データを生成する手段と、
遠隔地で前記生物測定データと前記公開鍵とを記憶する手段と、
前記復号鍵によって暗号化された前記生物測定データを含む前記ユーザ要求を局所で生成する手段と、
前記遠隔地に前記ユーザ要求を伝送する手段と、
前記遠隔地で前記公開鍵を用いて前記ユーザ要求を前記生物測定データに解読する手段と、
前記記憶された生物測定データを検索する手段と、
前記ユーザ要求を認証するために前記生物学的測定データを確認する手段と、を有することを特徴とする装置。
【請求項１２】前記生物学的測定データを確認する手段は、前記解読されたユーザ要求に送られた前記生物測定データと前記記憶された生物測定データとを比較する手段を含むことを特徴とする請求項１１に記載の装置。
【請求項１３】前記ユーザ要求を伝送する手段は、前記局所と前記遠隔地とを相互接続するネットワーク上であることを特徴とする請求項１２に記載の装置。
【請求項１４】前記復号鍵に対応付けられたＩＤ番号を持つ前記遠隔地の前記復号鍵を記憶する手段を、さらに有することを特徴とする請求項１３に記載の装置。
【請求項１５】前記ＩＤ番号は前記公開鍵に対して一意的に対応付けされており、前記装置はさらに、
前記ＩＤ番号および前記公開鍵を前記遠隔地の第１のデータベースに組として記憶する手段を有することを特徴とする請求項１４に記載の装置。
【請求項１６】前記生物測定データを前記遠隔地で第２のデータベースに記憶する手段をさらに有することを特徴とする請求項１５に記載の装置。
【請求項１７】前記ユーザおよび前記生物測定データに対応付けられたデータ・フィールドを生成する手段と、
前記生物測定データと前記データ・フィールドとを組として前記第２のデータベースに記憶する手段と、
をさらに有することを特徴とする請求項１６に記載の方法。
【請求項１８】前記復号鍵の記憶は、前記局所で行われることを特徴とする請求項１７に記載の装置。
【請求項１９】前記生物測定データの生成は、前記局所で行われることを特徴とする請求項１８に記載の装置。
【請求項２０】前記確認に応じて前記要求を処理する手段をさらに有することを特徴とする請求項１９に記載の装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータ・システムのセキュリティ技術、特に遠隔地からの要求およ

びメッセージを認証するための認証機構に関し、特に認証を行うための方法、装置、およびコンピュータ・プログラム・プロダクトに関する。

【０００２】

【従来の技術】公開／復号鍵対およびユーザＩＤ／パスワードはコンピュータ・システムの認証スキームで現在用いられている現代認証機構の基本的側面である。これらの基本的側面は、特定の一本のソフトウェア、例えばよく知られているLotus Notes（IBM Corporationの登録商標）アプリケーションまたは安定したウェブ・ブラウザによって使用されるハードウェアに存在しているデジタル証明書を介して元来特定のデバイスに結びつけられている。ハードウェア・セキュリティに穴があけられないようにセキュリティの層を追加するために、しばしばユーザＩＤおよびパスワードが使用される。特定のデバイスの物理的使用とユーザＩＤおよびパスワードについての認識との組み合わせは、過去においてユーザの認証を保証するのに十分なものと見なされていた。

【０００３】しかし、セキュリティに穴を開けるためのますます高度化する技術および情報に耐えようとする現代のセキュリティ・システムに対する絶え間ない攻撃によって、今ではそのようなシステムの機能が十分満足できるものではないことが嘆かわしいほどに明らかになった。例えば、万一ユーザＩＤおよびパスワード・データの信用が損なわれはじめ、またデバイスが公然とアクセス可能あるいは容易に紛失または盗難されやすくなると、例えばパーソナル・コンピュータまたはパーソナル・デジタル・アシスタント（ＰＤＡ）の場合、不正な使用によってユーザの権利が悲惨な結果となる。

【０００４】

【発明が解決しようとする課題】したがって、公用設定で実施される安全なトランザクションを可能とするために、特に普及しているデバイス、例えば前述のＰＤＡ、自動窓口機（ＡＴＭ）、キオスク等の様々な専用ネットワークあるいは公用ネットワーク、企業や他の事業実体のあいだで好評を博して展開されているイントラネットまたはインターネットそれ自体等を介して、そのような驚異を防ぐことができる技術の適用が緊急に求められている。

【０００５】

【課題を解決するための手段】適当なデバイスには、公開／復号鍵対が割り当てられ、また製造業者における指紋スキャニング・パッド等の生物測定データ入力デバイスが備え付けられている。指紋や網膜などの生物測定データは、ユーザの身元を確認するために、ネットワーク・コンピュータ、キオスク、パーソナル・デジタル・アシスタント（ＰＤＡ）および自動窓口機（ＡＴＭ）等の一般的なデバイスのユーザＩＤおよびパスワードに取って代わるものである。生物測定学的情報や現金の引き出しまたはクレジット・カードによる購買等のサービスに対する要求は、ネットワークに割り当てられた普遍的な管理されたアドレス（ＵＡＡ）と同様に、固有のデバイスＩＤに沿って製造業者のデバイスに割り当てられた復号鍵によって暗号化され、デバイスＩＤおよびメッセージ・ヘッダによって上流の信用サーバに転送される。サーバでは、生物測定データおよびサービス要求がデバイスの公開鍵によって解読される。このデバイスの公開鍵は、メッセージからのデバイスＩＤを用いて得られる。続いて、網膜スキャン、指紋等の転送されるタイプの事前に保存された生物学的データのデータベースに対して確認される。ひとたびユーザが認証されサービス要求がユーザの特権に対して確認されると、サーバは実行依頼された要求を安全に処理する。

【０００６】

【発明の実施の形態】図１は、本発明にもとづく強化されたセキュリティ・システムを構築するために、遠隔地および局所の両方で使用することが可能なコンピュータ・システムの一実施形態例を示す。このシステムは、ＣＰＵ１０、読み出し専用メモリ（ＲＯＭ）１１、ランダム・アクセス・メモリ（ＲＡＭ）１２、Ｉ／Ｏアダプタ１３、ユーザ・インタフェース・アダプタ１８、通信アダプタ１４、およびディスプレイ・アダプタ１９を有し、これらすべては共通のアドレス／データおよび制御バスまたはバス１６を介して相互に接続している。上記構成要素の各々は当業者に既知の従来の技術を用いて共通バスにアクセスし、バスマスタであるＣＰＵ１０によってシステム内の各構成要素に対して特定のアドレス範囲を提供するような方法が含まれる。図１にさらに示すように、ＤＡＳＤ１５等のそれらの外部ディバイスは、それぞれのアダプタ、例えばＩ／Ｏアダプタ１３を介して共通バス１６に接続する。他の外部ディバイス、例えばディスプレイ２１は、同様にディスプレイ・アダプタ１９等のそれぞれのアダプタを使用してバス１６とディスプレイ２１または他のデバイスとの間にデータ・フローを与える。様々なユーザ・インタフェース手段がユーザ・インタフェース・アダプタ１８との相互接続または利用のために提供され、図ではジョイ・スティック２３、マウス２５、キーボード１７、およびスピーカおよび（または）マイクロフォン２７等のそれぞれのユーザ入力デバイスに接続されている。システムは、１つ以上のアプリケーション３１の実行に適応した従来のオペレーティング・システム２９をさらに有する。これらのユニットの各々はそれ自体では当業者によく知られたものであることから、ここでの説明は省略する。

【０００７】本発明は、本質的に任意のコンピュータ・システムおよび対応するマイクロプロセッサの実現を認める。例えば、ＲＳ／６０００（登録商標）、ＲＩＳＣベース・ワークステーション、ＡＩＸ（登録商標）およびＯＳ／２（登録商標）オペレーティング・システムを各々実行するIBM Corporationのパーソナル・コンピュ

ータ、あるいは他のベンダーによる類似のハードウェアで、例えばＲＳ／６０００ワークステーションの場合は６０４ＰｏｗｅｒＰＣ（登録商標）ＲＩＳＣチップである（ＲＳ／６０００、ＩＢＭ、ＡＩＸ、ＯＳ／２およびＰｏｗｅｒＰＣはIBM Corporationの登録商標である）。

【０００８】図１のＣＰＵ１０と一緒に実装されているものは、一般にシステム・アドレス、データ、および図１のシステムの動作を補正するために必要な制御処理機能を実行する１つ以上のマイクロプロセッサである。本発明は様々なマイクロプロセッサ設計に対する適用を認めるが、ここに開示する実施形態例では、マイクロプロセッサはIBM Corporationによって製造されたＰｏｗｅｒＰＣ６０４マイクロプロセッサの形態をとる。このマイクロプロセッサは、縮小命令セット・コンピュータ（ＲＩＳＣ）マイクロプロセッサとして知られているマイクロプロセッサの一種である。そのようなマイクロプロセッサのアーキテクチャおよび動作についての詳細は、ＰｏｗｅｒＰＣ６０４ＲＩＳＣマイクロプロセッサの取扱説明書（PowerPC 604 RISC Microprocessor Users Manual, Document #MPC604UM/AD, Novermber, 1994, copyright IBM Corporation）（この文献を本明細書の記載の一部として援用する）から得ることができよう。

【０００９】本発明によれば、ユーザは、マウスおよび音声起動ナビゲーション等の様々なポインティング・デバイス２５によって操作可能であるディスプレイ２１上のカーソルおよびポップ・アップまたはポップ・ダウン・メニュー当の様々なオブジェクトを見るであろう。動作環境やＲＡＭ１２および（または）ＤＡＳＤ１５に常駐するアプリケーション・コードと関連してポインティング・デバイス２５およびマイクロフォン２７のためのデバイス・ドライバによってユーザ・インタフェース・アダプタ１８に対応付けられたプログラム・コードは、マイクロフォン２７に向かって話された相関的な音声コマンドに反応して、あるいは該音声コマンドと連携してディスプレイ・スクリーン２１上のカーソルの動きを促進かつ可能とさせる。

【００１０】図１のコンピュータ・システムに描かれた機能的構成要素を上記したように変更したり、以下に詳細に説明するローカル・デバイスおよびリモート・コンピュータ・システムの必要性および適用に適合させてもよい。例えば、ローカル・デバイスが既に述べたＰＤＡの形態を取る場合、ジョイスティックまたはスタンドアローン型のマウスまたは他のポインティング・デバイスは不要であるか、あるいはＰＤＡそれ自体のなかに組み込まれる。同様に、ＰＤＡの内蔵部品としてスタンドアローン型のディスプレイは不適当であり、またＬＣＤまたは他の小さなディスプレイはより妥当であることが認められよう。逆に、キオスクまたはＡＴＭ用途では、例えばそのようなスタンドアローン型のディスプレイがより妥当であろう。しかし、基本的な概念は、図１の機能的構成要素を異なる形態で、あるいは必要に応じてそのような構成要素を多数必要とするかもしれない遠隔地および局所の両方でかなり多様な異なるコンピューティング・デバイスを本発明では認められるということである。したがって、本発明はいかなる特定のコンピュータ・システムに限定されるものではない。

【００１１】ここで図２を再び参照しながら説明する。安全なトランザクションがもたらされるように図３のシステムによりエンド・ユーザによる使用のために製造業者がリモート・デバイスを準備してもよいかたちで以下説明する。そのような安全性を確保するために、そのような図はさらに図３のシステムで用いられるＩＤおよび鍵の生成をさらに詳細に説明する。

【００１２】第一に、当業者によく知られているいくつかの方法のいずれかによって、複数の公開／復号鍵対４０を生成するためのプロセスが用いられよう。同様に、プロセス４６は複数のデバイスＩＤを生成するために用いられよう。複数のデバイスＩＤは、図３のシステムと相互作用するリモート・ユーザによって用いられる異なった固有の物理的デバイスに各々が対応している。固有のデバイスＩＤは、一般にネットワーク・サーバやクライアントで用いられているネットワーク・インフォメーション・カード（ＮＩＣ）に対応付けられた普遍的な管理アドレス（ＵＡＡ）として知られているものと類似しているだろう。それによって、各個の物理的デバイス（例えば、ＮＩＣ、ＰＤＡ、ＡＴＭ、キオスク等）はそれ自体に対応付けられたそのようなデバイスＩＤを持つ。公開／復号鍵対生成プロセスからのフローは公開鍵矢印４２で示される公開鍵と復号鍵矢印５０で示される復号鍵となる。同様に、デバイスＩＤ生成プロセス４６からのフローは矢印４８および５２で示されるデバイスＩＤとなる。プロセス４０および４６からのフローしたＩＤ／公開鍵としての参照符号４４で示される公開鍵－デバイスＩＤ対は、矢印４５で模式的に示されるように、以下に記載するように暗号化鍵データベース７２（図３）に送られる。データベース７２は、各々が複数の個別のデバイスの異なる１つに対して一意的である複数のそのようなＩＤ／公開鍵対４４を格納する。

【００１３】同様に、プロセス４０および４６は、復号鍵矢印５０で示される複数の復号鍵とデバイスＩＤ矢印５２で示されるデバイスＩＤとを生成する。そのような固有の復号鍵／ＩＤ対は復号鍵／ＩＤ対５４として図示されている。復号鍵／ＩＤ対５４は矢印５６として示されるように送られ、また特に好ましくは暗号化プロセッサ・アセンブリ５８の一部分を含む読み取り専用メモリ（ＲＯＭ）６０上に付される。各々のそのような暗号化プロセッサ・アセンブリ（ＥＰＡ）５８によって、特定のＥＰＡ５８にのみ対応付けられた異なる固有のそのような復号鍵／ＩＤ対５４を不揮発的に保持することを容

易に理解することができよう。さらに、各ＥＰＡ５８は適当な生物測定学的入力センサ・デバイス６２と対応付けられる。このセンサ・デバイス６２は指紋スキャニング・パッド、網膜または顔スキャニング・カメラ等の形をとってもよく、例えば本発明によって認証される使用を行うＥＰＡ５８の特定のユーザに一意的に対応付けられた生物測定データを生じさせることが可能な任意のデバイスである。したがって、本発明は生物測定学的入力センサ・デバイスのいずれかの特定の形状に限定しようとするものではなく、むしろ特定のユーザに一意的に対応付けされ生物測定データの生成を行うことが可能な一切のデバイスによる用途を認めるものである。ＥＰＡ５８および生物測定学的入力センサ・デバイス６２は製造元によって一緒に結合させてもよく、あるいはエンド・ユーザ・デバイス、例えばＡＴＭ、キオスク、ＰＤＡ等を製造する際に必要に応じて接続してもよいことは理解されよう。ちなみに、「公開」および「復号」鍵は対となった鍵の固有の異なる部分に対してのみ使われる用語であることにさらに注目しておくべきであろう。ＥＰＡ５８のデバイス・オペレータは「公開」鍵のみにアクセスすることが理解されよう。

【００１４】ＩＤ、公開／復号鍵の生成についての説明、そのような復号鍵とＩＤＳとを用いるデバイスがリモート・ユーザによって使用されることを説明してきた。ここで、ＥＰＡと生物測定学的入力センサ・デバイスからの入力およびそれらのＩＤ／公開鍵対４４を用いる図３のシステムについてより詳細に説明する。

【００１５】はじめに、図３の上側には前述した暗号化鍵データベース７２が図示されている。このデータベース７２は図２で生成された複数のＩＤ／公開鍵対４４のためのリポジトリである。また、図３の下側部分には、既におなじみのＰＤＡ５８が図示されている。このＰＤＡ５８はＲＯＭ６０を有するもので、図２のプロセスにもとづいて生成され、かつ特定のＥＰＡ５８に一意的に対応付けられた復号鍵／ＩＤ対の１つが格納されている。

【００１６】さらに図３では、生物測定学的鍵データベース７４が表示されている。このデータベース７４は、複数の生物測定データーユーザ・データ・フィールド対からなる。そのような対の各々では、生物測定データは特定のエンド・ユーザに一意的に対応付けられており、さらに許可、アカウント番号等の複数のデータ・フィールドもまた特定のエンド・ユーザに一意的に対応付けられており、エンド・ユーザの生物測定データはすべてデータ・ベース７４に格納される。

【００１７】図３のシステムは、さらに信用サーバ７０を含む。このサーバ７０の一部分は、ユーザのＥＰＡ５８とのユーザ・インタラクションによって送出されたエンド・ユーザ要求に応える機能を果たす。信用サーバ７０とＥＰＡ５８との間に配置された適当なネットワーク６６によって、ＥＰＡ５８と信用サーバ７０とが互いに通信しあう。このネットワークはイントラネット、インターネット、ダイアル・アップ・ネットワーク、あるいはリモートＥＰＡ５８とサーバ７０とが相互接続するのに適した適当な他のネットワークのいずれかの形をとるものであってもよい。

【００１８】信用サーバ７０によって実行される本発明に関係した１つの重要な機能は、データベース７２に格納された暗号化鍵を用いてＥＰＡ５８によって生成された要求６４を解読し、データベース７４に格納された生物測定データを介してユーザ許可および他のデータを認可する機能を提供することである。以下に詳細に説明するこのような要求６４は、ＲＯＭ６０に格納されたデバイスＩＤデータ５４および他のトランザクション・データのいずれかと同様にセンサ・デバイス６２を介したユーザ入力の生物測定データを含む。このＩＤ、生物測定データおよびトランザクション・データはサーバ７０へのリンク６８を介してネットワーク６６に送られる。２方向矢印７６および７８でそれぞれ示されるデータベース７４とデータベース７２との相互作用は、より詳細に説明されるであろう方法によってライン６８を通って入ってくる暗号化されたユーザ要求の解読を生ずる。

【００１９】したがって、以上のことをまとめると、ＥＰＡ５８と対話するユーザは本質的に、特定のＡＴＭ、キオスク、ＰＤＡ等にある生物測定学的入力センサ・デバイス６２を用い、ＥＰＡ５８によって表されるユーザの生物学的入力データを提供する。ユーザは、このように存在する生物測定データに基づいてさらに使用する確認を要求する。そのような生物測定データは、従来技術にもとづくものであろうとなかろうと損なわれやすい（例えば、悪事を行う者が正当なユーザの指紋を盗むこと等）ので、本発明の重要な特徴は特定のＥＰＡ５８でこの不適当な生物測定データを使用する能力に欠けている悪事を行う者によってそのようなデータが使用されることはほとんどないので、このデータはＲＯＭ６０に格納された復号鍵５４によってさらに暗号化され、特定のユーザに一意的に対応付けられるであることに注目することが重要である。

【００２０】データベース７２および７４に格納されている情報を用いるサーバ７０によってひとたび解読が実行されると、確認が実行されたエンド・ユーザへの通知はサーバ７０からネットワーク６６へ向けてライン６９上を送られ、最終的にネットワーク６６からＥＰＡ５８へのライン７１で示されるようにＥＰＡ５８を経由してエンド・ユーザに送られてもよい。その後、安全なリンクがそれによって確立され、エンド・ユーザはサーバ７０と対話するように詳細を追加してもよく、それによってデータベース７４のユーザ・データ・フィールドへのデータの追加を行ったり、あるいは必要に応じて特定のユーザに対応付けられたそのようなデータの検索を許可

したりすることも可能である。

【００２１】確認機能決定ブロック８０はさらに図３に示されており、有効な要求が存在するかどうかを決定するために、データベース７２内の対応するＩＤ／公開鍵情報およびデータベース７４内の生物測定データとライン６４上を入ってくる復号鍵／ＩＤ情報を相関させることに使用される可能性がある一連の論理プロセスを機能的に表現する。したがって、本発明は確認機能決定アルゴリズム８０のいかなる特定の形に限定されるものではなく、本質的にそれらの入力を適当なものとして用いるいかなる決定も許容する。入力はライン８２によって確認機能決定ブロック８０へ送られるものとして示されて、それからもたらされる最終的な決定は確認機能決定ブロック８０からライン８６を経由してサーバ７０に戻る。

【００２２】ここで図４に戻る。この図４に描かれているのは、ＥＰＡ５８を生成するのに用いられる一連のイベントを説明し、図２に関連して既に説明したような方法で生成される様々な鍵およびＩＤを生じさせるフローチャートである。最初に、図２の鍵生成プロセッサ４０に対応して参照ブロック８８で示される各々の潜在的なユーザに対して、鍵の対K_1、K_2が生成されることが再現されるだろう。同様に、複数の特有のデバイスＩＤが生成され、各々が異なる物理的ＥＰＡ５８に対応し、そのようなデバイスＩＤの生成はブロック９０として示され、さらに図２のブロック４６に対応する。その結果、複数のＩＤ、K_1からなる対と、複数のK_2対を生成するために、生成されたこれらの鍵の対と特有のデバイスＩＤは矢印９２および９４とブロック９６とに示すように結合する。ＩＤのK_2対はライン１１４に示すように送られ、引き続いて起こるＥＰＡ５８の購入者への転送のために暗号化鍵データベース７２に格納される。ＩＤ、K_2対の格納はブロック１１６に示される。デバイス・オペレータがＥＰＡ５８を獲得あるいは購入した場合、一意のＩＤ、K_2対が送られ、ブロック１２０のライン１１８で示すように、または最終結合デバイス・オペレータに送られ、そこからライン１２２で示すように、IDK_2対はブロック１２４で示される様々なＩＤで鍵がかけられたデータベース７２に置かれる。このようにして、ＥＰＡに対応する特定のＥＰＡ５８をエンド・ユーザが用いる場合、データベース７２に常駐する一意的なＩＤと公開鍵とが存在する。

【００２３】図４を参照しながらさらに説明する。IDK_2対と同じようにして、IDK_1対は矢印９８に模式的に示したように、一意的に対応付けられたＥＰＡ５８に送られ、それによってIDK_1は特定のＥＰＡ５８上のＲＯＭ６０に書き込まれる。このことは図４のブロック１００で示されている。このIDK_1対がＲＯＭ６０に「書き込まれる（burned）」と表現されるのに対して、重要な点は特定のＥＰＡ５８に一意的に対応付けられたIDK_1データはＥＰＡ５８に不揮発的に格納されることである。したがって、本発明は、このような目標に達成するために数多くの様々な方法のいずれかを許容するもので、その中のほんの１例としてフラッシュ・バイオス、E^2ＰＲＯＭ、ソケットにはめられたＲＯＭの物理的交換等によって実際に「書き込む（burn）」。

【００２４】図４を参照しながらさらに説明する。ひとたびこのIDK_1データが特定のＥＰＡ５８に関連して不揮発的に格納されると、プロセスはフロー１２０によって示されるように続行し、この特定のＥＰＡ５８が選択される生物測定学的入力デバイス６２と結合され、そのような結合は図４においてブロック１０４として表される。この結合は、例えば、生物測定学的入力デバイス６２と対話する特定のユーザに関する生物測定データとＲＯＭのデータ（例えば、復号鍵／ＩＤ対５４）とを含む電気的に生じた要求を提供することが可能なように、電気的およびソフトウェア的に、ＲＯＭ６０と生物測定学的入力センサ・デバイス６２とが統合されることのみを意味する。

【００２５】ひとたびこのＥＰＡと生物測定学的入力デバイスとがそのように電気的に「結合（coupled）」されてアセンブリを形成すると、該結合アセンブリは前述したＡＴＭ、キオスク、ＰＤＡ等であろうとなかろうと適当な末端デバイス１０８に取り付けられ、かつ該デバイス１０８とアセンブルされる。

【００２６】最後に、フロー１１０によって示されるように、キオスクをショッピング・モールに据え付けたり、ＡＴＭ機械をドライブ・スルー・バンクに据え付けたり、ＰＤＡをエンド・ユーザに販売したりするなど、このような所望のデバイスに設けられた結合アセンブリの配置を行う。

【００２７】ここで図５を参照しながら説明する。この図は、図３に示されたシステムのトランザクション許可の流れを説明するためのフローチャートである。ここでは、上記したような様々な鍵、ＩＤ、データベースおよびＥＰＡが使用され、エンド・ユーザはネットワーク６６を介してサーバ７０にトランザクションを生成し、安全な許可を受け取ることが可能である。はじめに、使用中、デバイス・オペレータによって生物測定データを同様の生物測定学的入力センサを介して登録するために、ユーザはＥＰＡのオペレータと対話する。ひとたび登録されると、使用中、ユーザは適当な生物測定データを入力（１２６）、ＥＰＡ（網膜スキャナ、指紋スキャナ等）を付属する特定のトランスデューサによってもろん制御され、フローが継続する。フローは矢印１２８に沿ってブロック１３０へと続く。ブロック１３０で示されるこの地点で、オペレータは、既に述べた関連記録データ（例えば、アカウント番号、許可等の既に指摘したデータ・フィールド）に沿って第２または生物測定データベース７４の鍵としてブロック１２６にもとづいて、そ

のようにして得られた生物測定データを利用する。フローは、さらに矢印１３２に沿ってブロック１３４に続く。このブロック１３４では、ユーザはトランザクション許可を要求するように生物測定データ入力デバイスに結合したＥＰＡを用いる。つぎに、フローは矢印１３６に沿ってブロック１３８に続く。このブロック１３８は入力生物測定データとトランザクション・データとの組み合わせを第１の鍵K_1を用いて暗号化されたメッセージのなかに表す。

【００２８】図５を参照しながらさらに説明する。フローは矢印１４０に沿ってブロック１４２に続く。このブロック１４２は、ＥＰＡ５８のシステムがその後、ＲＯＭ６０に格納されたＩＤをクリア・テキストで要求メッセージに付加するという意味を表す。フローは矢印１４４に沿ってブロック１４６に続く。このブロック１４６は、その後の解読のために、そのようにコンパイルされたメッセージが要求６４としてネットワーク６６介し、かつコネクション６８によってサーバ７０へ送られることを示す。

【００２９】フローはつぎに矢印１４８に沿ってブロック１５０に続く。このブロック１５０は機能的に信用サーバ７０を表すもので、ＥＰＡＩＤをはがし、それをデータベース７２に対応付けられたユーザの鍵K_2の検索に用いる。ひとたびこのことが完了すると、フローは矢印１５２に沿って続き、ブロック１５４で、この鍵K_2は既に記載されたブロック１３８に従ってK_1メッセージによって事前に暗号化されているメッセージを解読するのに使われる。フローは矢印１５６に沿ってブロック１５８に続く。このブロック１５８は、確認機能８０にその後に要求されたメッセージが送られることを示す。フローは矢印１６０に沿ってブロック１６２に続く。このブロック１６２は、生物測定データベース７４からのユーザ・データを検索するために鍵としてメッセージの生物測定学的部分を用いる確認機能のステップを示す。フローは矢印１６４に沿ってブロック１６６に続く。このブロック１６６では、確認機能８０は矢印８２に沿ってサーバ７０から受け取ったこのデータに基づいて認証決定を下す。確認機能はK_2鍵による場合と同様に任意に応答を暗号化して、矢印８６に示されるように元のデバイスに送り戻すことが可能であるという点が注目されよう。つぎにフローは矢印１６８に沿ってブロック１７０に続く。このブロックは、サーバ７０の機能を表すもので、その後、確認されている要求の結果としての応答をネットワーク６６を通してＥＰＡ５８を用いるエンド・ユーザに送る。そこで応答を、既知のK_1鍵で任意に解読（ステップ１６６で暗号化されている場合）することができると、デバイス５８はこの認証決定データに作用することが可能であろう。

【００３０】本発明の真の精神から逸脱することなく本発明の好ましい実施形態例に種々の修飾または変化を加えることが可能であることは上記の説明から理解されよう。この発明の詳細な説明の記載が説明することのみを目的として記述されたもので、限定的な意味で解釈されるべきではないことが意図されている。この発明の範囲は特許請求の範囲によってのみ限定される。

【００３１】まとめとして、本発明の構成に関して以下の事項を開示する。

（１）コンピュータ・システム・ネットワークでユーザの要求を認証するための方法であって、復号鍵および公開鍵を生成するステップと、前記ユーザに対応する生物測定データを生成するステップと、遠隔地で前記生物測定データと前記公開鍵とを記憶するステップと、前記復号鍵によって暗号化された前記生物測定データを含む前記ユーザ要求を局所で生成するステップと、前記遠隔地に前記ユーザ要求を伝送するステップと、前記遠隔地で前記公開鍵を用いて前記ユーザ要求を前記生物測定データに解読するステップと、前記記憶された生物測定データを検索するステップと、前記ユーザ要求を認証するために前記生物学的測定データを確認するステップと、を有することを特徴とする方法。

（２）前記生物学的測定データを確認するステップは、前記解読されたユーザ要求に送られた前記生物測定データと前記記憶された生物測定データとを比較することを含むことを特徴とする上記（１）に記載の方法。

（３）前記ユーザ要求の伝送は、前記局所と前記遠隔地とを相互接続するネットワーク上であることを特徴とする上記（２）に記載の方法。

（４）前記復号鍵に対応付けられたＩＤ番号を持つ前記遠隔地の前記復号鍵を記憶するステップを、さらに有することを特徴とする上記（３）に記載の方法。

（５）前記ＩＤ番号は前記公開鍵に対して一意的に対応付けされており、前記方法はさらに、前記ＩＤ番号および前記公開鍵を前記遠隔地の第１のデータベースに組として記憶するステップを有することを特徴とする上記（４）に記載の方法。

（６）前記生物測定データは第２のデータベースに記憶されていることを特徴とする上記（５）に記載の方法。

（７）前記ユーザおよび前記生物測定データに対応付けられたデータ・フィールドを生成するステップと、前記生物測定データと前記データ・フィールドとを組として前記第２のデータベースに記憶するステップと、をさらに有することを特徴とする上記（６）に記載の方法。

（８）前記復号鍵を記憶するステップは、前記局所で行われることを特徴とする上記（７）に記載の方法。

（９）前記生物測定データを生成するステップは、前記局所で行われることを特徴とする上記（８）に記載の方法。

（１０）前記確認に応じて前記要求を処理するステップをさらに有することを特徴とする上記（９）に記載の方法。

（１１）コンピュータ・システム・ネットワークでユーザの要求を認証する装置であって、復号鍵および公開鍵を生成する手段と、前記ユーザに対応する生物測定データを生成する手段と、遠隔地で前記生物測定データと前記公開鍵とを記憶する手段と、前記復号鍵によって暗号化された前記生物測定データを含む前記ユーザ要求を局所で生成する手段と、前記遠隔地に前記ユーザ要求を伝送する手段と、前記遠隔地で前記公開鍵を用いて前記ユーザ要求を前記生物測定データに解読する手段と、前記記憶された生物測定データを検索する手段と、前記ユーザ要求を認証するために前記生物学的測定データを確認する手段と、を有することを特徴とする装置。

（１２）前記生物学的測定データを確認する手段は、前記解読されたユーザ要求に送られた前記生物測定データと前記記憶された生物測定データとを比較する手段を含むことを特徴とする上記（１１）に記載の装置。

（１３）前記ユーザ要求を伝送する手段は、前記局所と前記遠隔地とを相互接続するネットワーク上であることを特徴とする上記（１２）に記載の装置。

（１４）前記復号鍵に対応付けられたＩＤ番号を持つ前記遠隔地の前記復号鍵を記憶する手段を、さらに有することを特徴とする上記（１３）に記載の装置。

（１５）前記ＩＤ番号は前記公開鍵に対して一意的に対応付けされており、前記装置はさらに、前記ＩＤ番号および前記公開鍵を前記遠隔地の第１のデータベースに組として記憶する手段を有することを特徴とする上記（１４）に記載の装置。

（１６）前記生物測定データを前記遠隔地で第２のデータベースに記憶する手段をさらに有することを特徴とする上記（１５）に記載の装置。

（１７）前記ユーザおよび前記生物測定データに対応付けられたデータ・フィールドを生成する手段と、前記生物測定データと前記データ・フィールドとを組として前記第２のデータベースに記憶する手段と、をさらに有することを特徴とする上記（１６）に記載の方法。

（１８）前記復号鍵の記憶は、前記局所で行われることを特徴とする上記（１７）に記載の装置。

（１９）前記生物測定データの生成は、前記局所で行われることを特徴とする上記（１８）に記載の装置。

（２０）前記確認に応じて前記要求を処理する手段をさらに有することを特徴とする上記（１９）に記載の装置。

【図面の簡単な説明】

【図１】ＰＤＡ等の一般的なリモート・デバイスからなる手段によって対話する本発明の具体化した部分であるリモート・コンピュータ・システムの高度に機能的なブロック図である。

【図２】リモート・ユーザ・デバイスが本発明にもとづいて構成される手順を説明するための機能的なブロック図である。

【図３】図２に示すデバイスによって本発明にもとづいて対話するリモート・システムの構成要素を表す機能的なブロック図である。

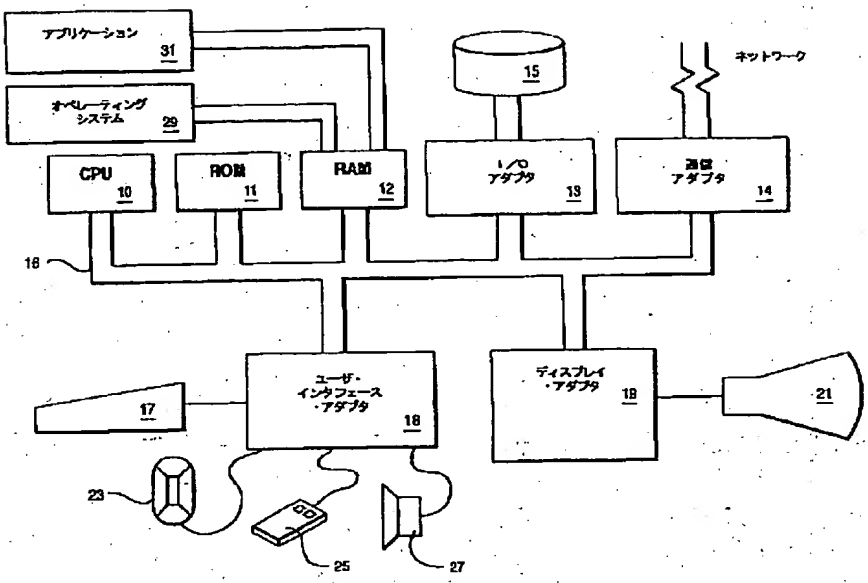
【図４】図２のリモート・ユーザ・デバイスが生成されるステップとセキュリティ情報を有する図３のシステムとを説明するためのフローチャートである。

【図５】所望の安全なトランザクション許可をもたらすように図２のデバイスが図３のシステムと対話する場合のイベントの順序を説明するためのフローチャートである。

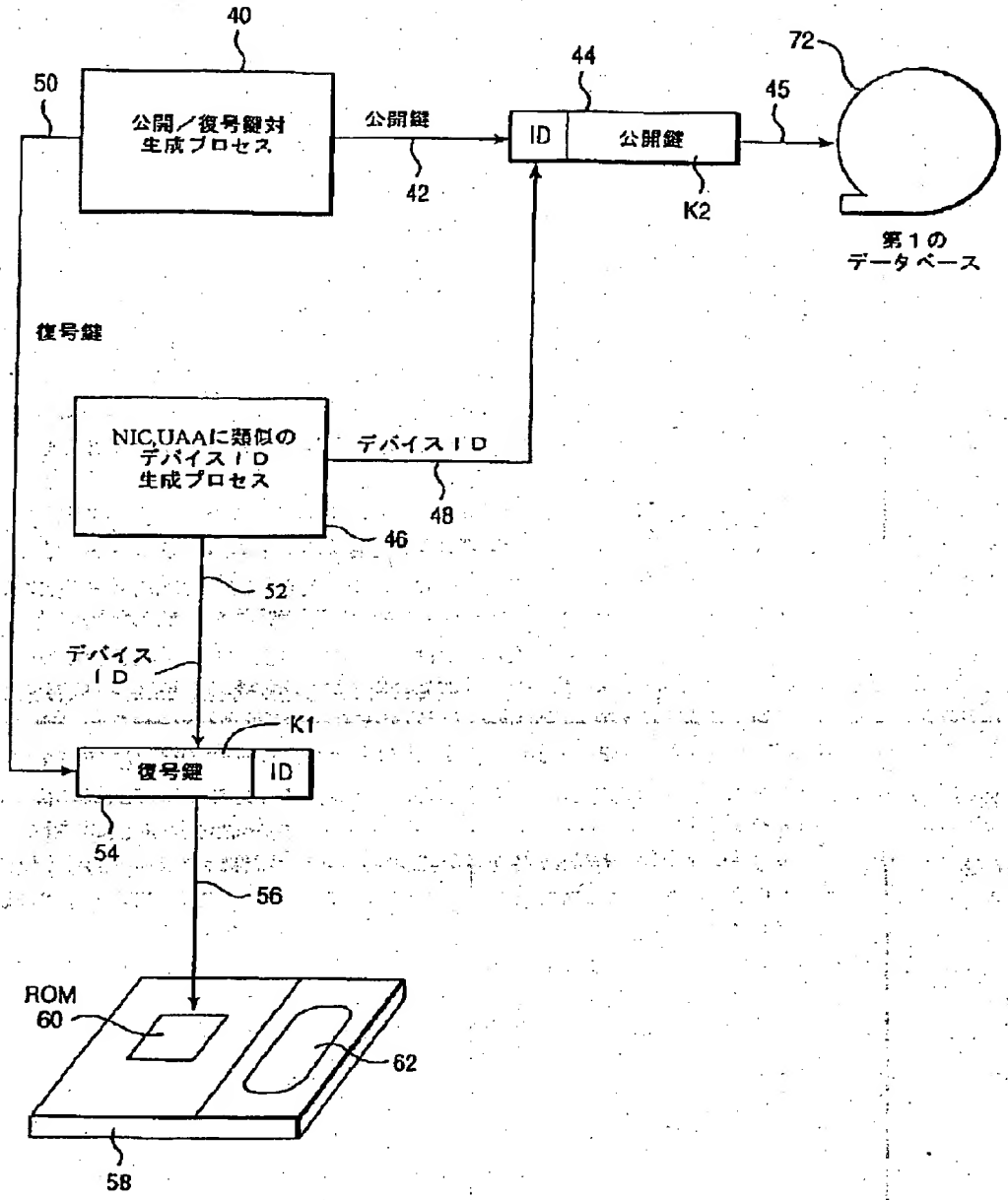
【符号の説明】

１０	ＣＰＵ
１１	ＲＯＭ
１２	ＲＡＭ
１３	Ｉ／Ｏアダプタ
１４	通信アダプタ
１５	ＤＡＳＤ
１６	バス
１７	キーボード
１８	ユーザ・インタフェース・アダプタ
２１	ディスプレイ（ディスプレイ・スクリーン）
２３	ジョイ・スティック
２５	ポインティング・デバイス（マウス）
２７	スピーカおよび（または）マイクロフォン
２９	オペレーション・システム
４０	公開／復号鍵対の生成プロセス
４２	矢印
４４	公開鍵－復号鍵対
４５	矢印
４６	デバイスＩＤ生成プロセス
４８	矢印
５０	矢印
５４	復号鍵－ＩＤ対
５６	矢印
５８	暗号化プロセッサ・アセンブリ（ＥＰＡ）
６０	ＲＯＭ
６２	生物測定学的入力センサ・デバイス
６４	要求
６６	ネットワーク
６８	リンク
７０	信用サーバ
７２	データベース
７４	データベース
７６	矢印
７８	矢印
８０	確認機能決定ブロック
８６	矢印

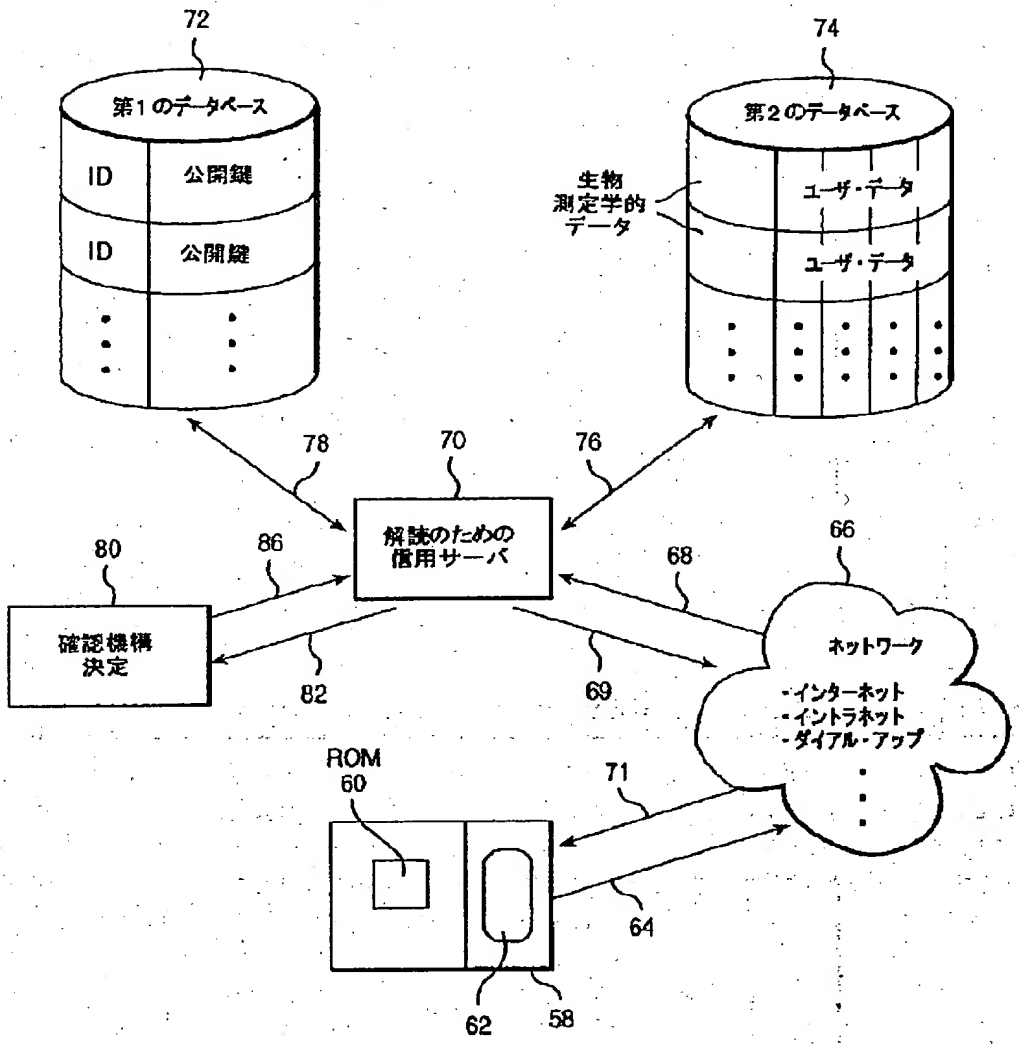
【図１】


アプリケーション
31
オペレーティング
システム
29
CPU
10
ROM
11
RAM
12
15
I/O
アダプタ
13
ネットワーク
通信
アダプタ
14
16
17
ユーザ・
インタフェース
・アダプタ
18
ディスプレイ
・アダプタ
19
21
23
25
27

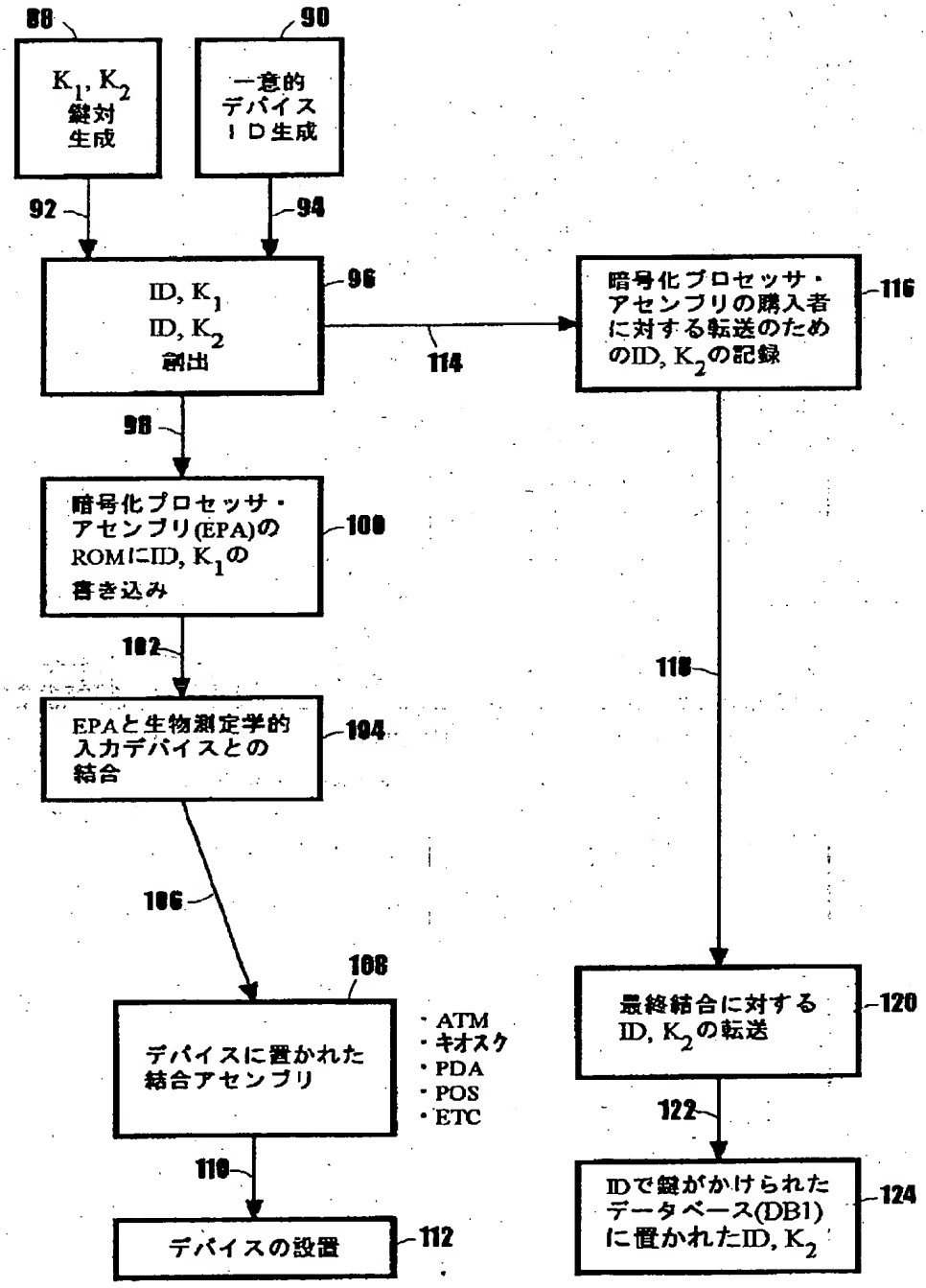
【図２】


40
50
公開／復号鍵対
生成プロセス
公開鍵
42
44
ID
公開鍵
K2
45
72
第１の
データベース
復号鍵
NIC,UAAに類似の
デバイスＩＤ
生成プロセス
デバイスＩＤ
48
46
52
デバイス
ＩＤ
K1
復号鍵
ID
54
56
ROM
60
62
58

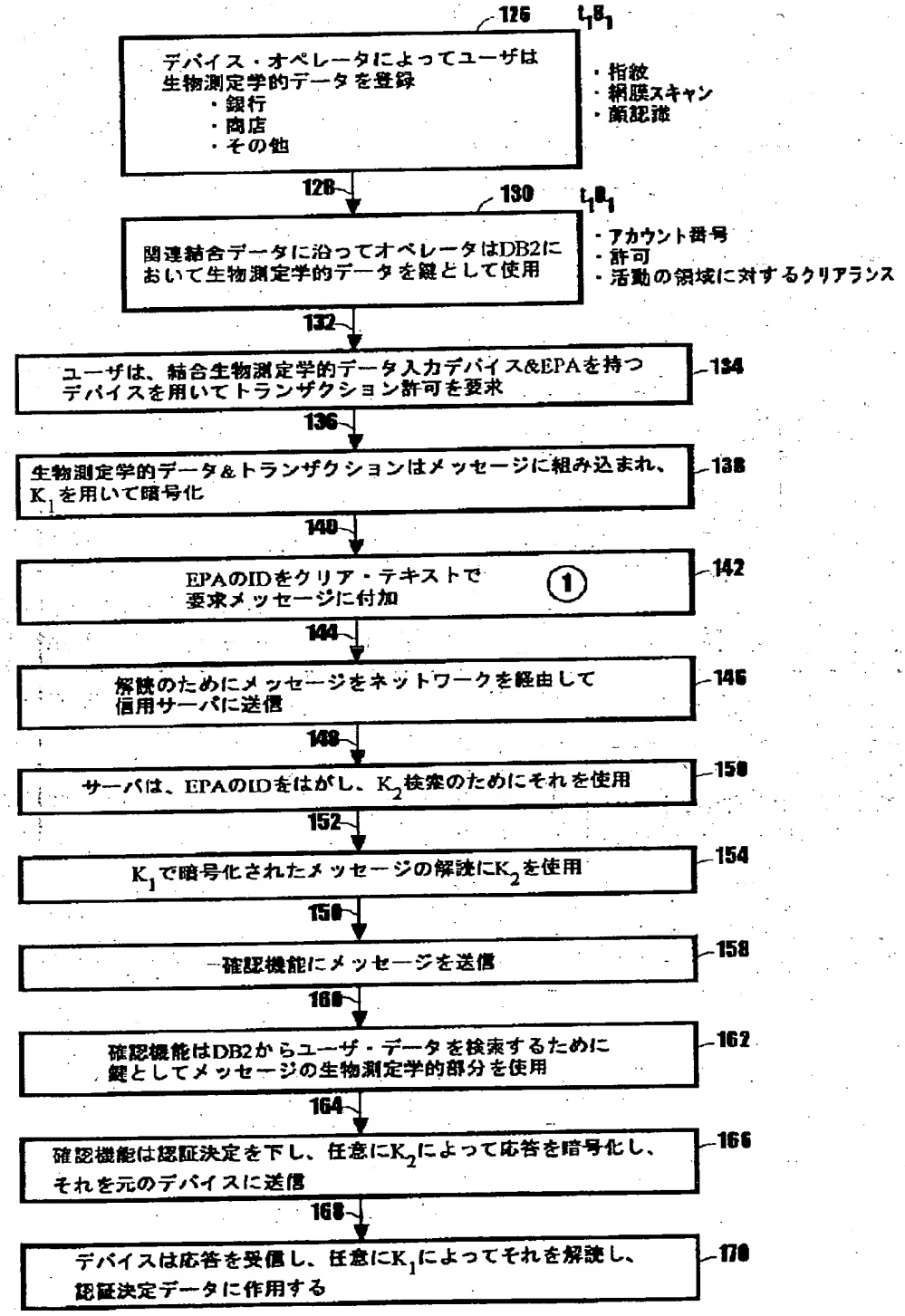
【図３】


72
第１のデータベース
ID
公開鍵
ID
公開鍵
74
第２のデータベース
生物
測定学的
データ
ユーザ・データ
ユーザ・データ
78
70
76
解読のための
信用サーバ
80
86
68
66
確認機構
決定
82
69
ネットワーク
・インターネット
・イントラネット
・ダイアル・アップ
ROM
60
71
64
62
58

【図4】


88
K_1, K_2 鍵対 生成
90
一意的 デバイス ID生成
92
94
ID, K_1 ID, K_2 創出
96
114
暗号化プロセッサ・アセンブリの購入者に対する転送のためのID, K_2の記録
116
98
暗号化プロセッサ・アセンブリ(EPA)のROMにID, K_1の書き込み
100
102
EPAと生物測定学的入力デバイスとの結合
104
118
106
108
デバイスに置かれた結合アセンブリ
・ATM
・キオスク
・PDA
・POS
・ETC
最終結合に対するID, K_2の転送
120
122
110
IDで鍵がかけられたデータベース(DB1)に置かれたID, K_2
124
デバイスの設置
112

【図5】


125
デバイス・オペレータによってユーザは生物測定学的データを登録
・銀行
・商店
・その他
・指紋
・網膜スキャン
・顔認識
126
130
関連結合データに沿ってオペレータはDB2において生物測定学的データを鍵として使用
・アカウント番号
・許可
・活動の領域に対するクリアランス
132
ユーザは、結合生物測定学的データ入力デバイス&EPAを持つデバイスを用いてトランザクション許可を要求
134
136
生物測定学的データ&トランザクションはメッセージに組み込まれ、K_1を用いて暗号化
138
140
EPAのIDをクリア・テキストで要求メッセージに付加 ①
142
144
解読のためにメッセージをネットワークを経由して信用サーバに送信
146
148
サーバは、EPAのIDをはがし、K_2検索のためにそれを使用
150
152
K_1で暗号化されたメッセージの解読にK_2を使用
154
156
確認機能にメッセージを送信
158
160
確認機能はDB2からユーザ・データを検索するために鍵としてメッセージの生物測定学的部分を使用
162
164
確認機能は認証決定を下し、任意にK_2によって応答を暗号化し、それを元のデバイスに送信
166
168
デバイスは応答を受信し、任意にK_1によってそれを解読し、認証決定データに作用する
170

フロントページの続き

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ	テーマコード（参考）
		Ｈ０４Ｌ　9/00	６７５Ｂ